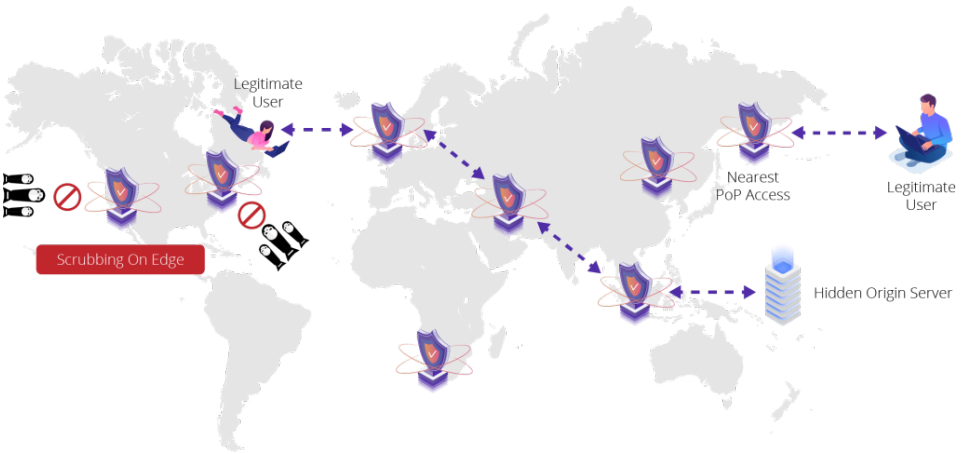
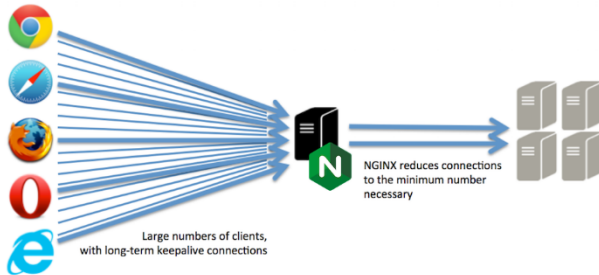
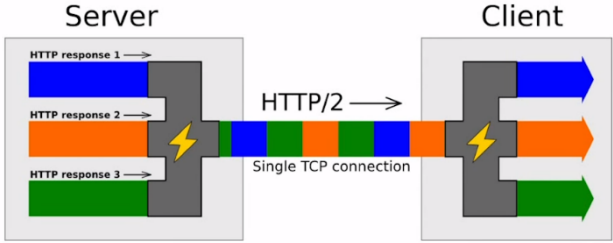


# EXHIBIT 2

### Claim Chart

| U.S. Patent No.<br>8,265,089   | CDNetworks Application Shield/Flood Shield  |
|--|---|
| <p>7. A gateway computer for use in a computer communication network system, the gateway computer comprising a non-transient software storage device with the following software encoded therein: a gateway module and an enhanced requesting module; wherein:</p> | <p>CDNetworks' network receives data packets from users on the internet. Data packets from a user enter the network through an edge router (a gateway computer) at a CDNetwork Point-of-Presence.</p> <p>CDNetworks has a network of over 200,000 servers and over 2,800 global Points of Presence (PoPs).<br/>See <a href="https://www.cdnetworks.com/">https://www.cdnetworks.com/</a></p>  <p>The diagram illustrates a global network map with various Points of Presence (PoPs) marked by shield icons. A 'Legitimate User' in North America sends data packets that travel through an edge router (labeled 'Scrubbing On Edge') and through multiple PoPs across Europe and Asia, eventually reaching a 'Hidden Origin Server' in Asia. Another 'Legitimate User' in Asia is shown sending packets through a 'Nearest PoP Access' point to the same hidden origin server. The map shows the distribution of these PoPs across the USA, Europe, Asia, and mainland China.</p> <p>See <a href="https://www.cdnetworks.com/cloud-security/flood-shield/">https://www.cdnetworks.com/cloud-security/flood-shield/</a></p> <p>“Flood Shield DDoS deflection technology is deployed on CDNetworks’ distributed Points-of-Presence (PoPs). It is a cloud-based ‘always-on’ mitigation service with virtually unlimited capacity.”<br/><a href="https://www.cdnetworks.com/cloud-security/flood-shield/">https://www.cdnetworks.com/cloud-security/flood-shield/</a></p> <p>“Flood Shield is deployed on CDNetworks’ huge global infrastructure with data centers in the USA, Europe, Asia, and mainland China. With over 12 global DDoS scrubbing centers and 15Tbps of total capacity, it is designed to protect websites and network infrastructures against even the most sophisticated and large-scale volumetric attacks.”<br/><a href="https://www.cdnetworks.com/cloud-security/flood-shield/">https://www.cdnetworks.com/cloud-security/flood-shield/</a></p> <p>“Flood Shield is deployed on CDNetworks’ distributed Points-of-Presence (PoPs). It is a cloud-based ‘always on’ solution with virtually unlimited capacity. It does not require sophisticated deployments and changes to customers’ network and provides automated transparent scaling. Flood Shield is provided either via a simple DNS change, typically to protect web sites and HTTP/S traffic, or through an anycast IP in order to protect entire network infrastructures, including multiple domains, servers</p> |

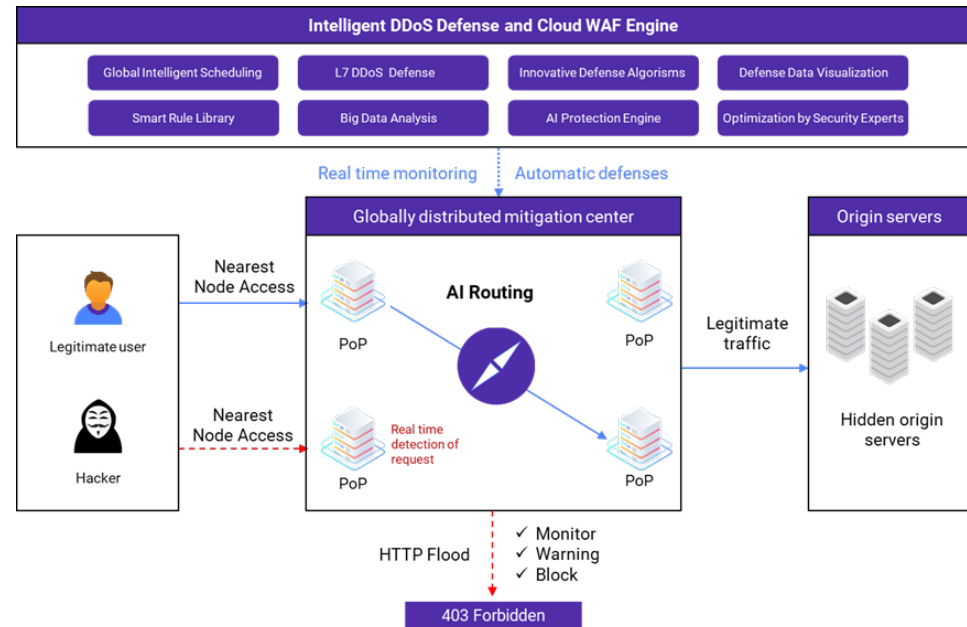
|   |  |
|---|--|
|   | <p>and protocols. With the customers' traffic routed through CDNetworks' PoPs, DDoS attacks hit the CDNetwork infrastructure rather than our customers' servers and networks. CDNetworks' PoPs detect and deflect both application-layer attacks (L7) and all known types of network-layer attacks (L3/L4), including Ack and Syn floods, UDP floods, ICMP floods, CC attacks and more."</p> <p><a href="https://documents.cdnetworks.com/document/15920/floodshield-how-it-work">https://documents.cdnetworks.com/document/15920/floodshield-how-it-work</a></p> <p>"Application Shield is a cloud-based WAF and DDoS protection solution, deployed on CDNetworks global Points-of presence (PoPs) to detect and defend against web attacks in real-time. This happens at the edge of the network, far before the attack can hit, manipulate, or overwhelm the customers' data centers and origin servers."</p> <p><a href="https://documents.cdnetworks.com/document/15921/appshield-howitworks?rsr=cdnw">https://documents.cdnetworks.com/document/15921/appshield-howitworks?rsr=cdnw</a></p> <p>CDNetworks has PoPs located in Ashburn, VA; Boston, MA; Chicago, IL; Dallas, TX; Denver, CO; Los Angeles, CA; Miami, FL; New York, NY; San Jose, CA; and Seattle, WA</p> <p>See <a href="https://www.cdnetworks.com/cdnpro-pricing/">https://www.cdnetworks.com/cdnpro-pricing/</a></p> |
| <p>the gateway module is structured, programmed and/or data-communication-connected to receive a first MPDU from a connection-based network of the computer communication network system, to disaggregate the first MPDU into a plurality of smaller data units (DUs), and selectively communicate the first DU to a receiver-side connectionless network of the computer communication</p> | <p>CDNetworks' edge routers receive packets (MPDUs) from the internet (a connection-based network), disaggregate/demux those packets into smaller packets (smaller DUs), and communicate the smaller packets to a target network (a receiver-side connectionless network).</p> <p>"CDN Pro is a serverless Nginx Platform with control at the Edge, built-in security, and real-time acceleration for optimizing websites, APIs, and cloud applications."</p> <p><a href="https://www.cdnetworks.com/cdnpro/">https://www.cdnetworks.com/cdnpro/</a></p>  <p><a href="https://www.nginx.com/blog/load-balancing-with-nginx-plus-part-2/">https://www.nginx.com/blog/load-balancing-with-nginx-plus-part-2/</a></p>   |

|   |   |
|---|---|
| <p>network system;<br/>and</p>  | <p style="text-align: center;">HTTP/2 Inside: multiplexing</p>  <p>“The next key point of HTTP/2 is multiplexing. Instead of sending and receiving responses and requests as separate streams of data over multiple connections, HTTP/2 multiplexes them over one stream of bytes or one stream of data.”<br/> <a href="https://www.nginx.com/blog/http2-module-nginx/">https://www.nginx.com/blog/http2-module-nginx/</a></p>  |
| <p>the enhanced requesting module is structured, programmed and/or data-communication-connected to collect selected network protocol data from the first MPDU, with the selected network protocol data including at least some network protocol data included in the first MPDU and not included in any of the plurality of DUs, and with the selected network protocol data relating exclusively to network protocols and including no data from any data payload(s) which may be present in</p> | <p>CDNetworks collects network protocol data, such as IP addresses, from incoming data packets received from the internet. None of this network protocol data includes data from the packet payload.</p> <p>“CDNetworks content delivery networks (CDN) serves thousands of large global enterprises, process TB-scale log data daily, including a massive access data and attack/defense samples. The platform’s big data and machine learning capabilities help detect network attack trends in real-time and automatically activates defense in advance. It also intelligently analyzes and identifies attacks, to model the normal behaviors of legitimate traffic including IP addresses, HTTP headers, cookies, and JavaScript snippets, etc.”<br/> <a href="https://www.cdnetworks.com/cloud-security/flood-shield/">https://www.cdnetworks.com/cloud-security/flood-shield/</a></p> <p><u>“Layer 4 DDoS Mitigation</u><br/> CDN Pro is built upon our Edge Computing Platform. At the entry point of every edge Point of Presence (PoP) is a high-performance Layer 4 distributed denial-of-service (DDoS) firewall. The firewall consists of a group of machines that analyze incoming traffic at line speed. Based on regularly updated rules, the firewall rejects suspicious packets that may endanger services and forwards only the ‘safe’ packets to the servers located behind the firewall. This feature is enabled by default for all edge services and is transparent to all the users.</p> <p><u>Layer 7 DDoS Mitigation</u><br/> The CDN Pro platform monitors the traffic in real-time to detect unusual behaviors at layer 7. Once an attack is identified, defense strategies will be deployed in both layer 4 and layer 7 to most effectively mitigate the impact to normal traffic. Since its inception, CDN Pro has successfully</p> |

the MPDU;

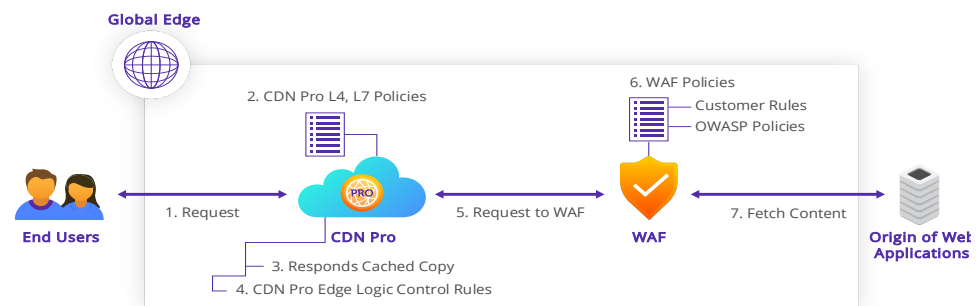
handled some of the world's largest DDoS attacks with bandwidth reaching 1.2Tbps and request rate as high as 35Mrps.”

<https://docs.cdnetworks.com/en/cdn/docs/recipes/secure-delivery>

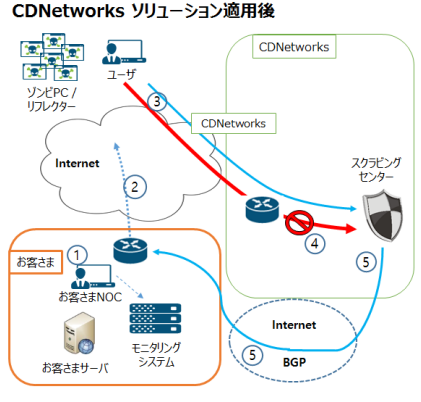


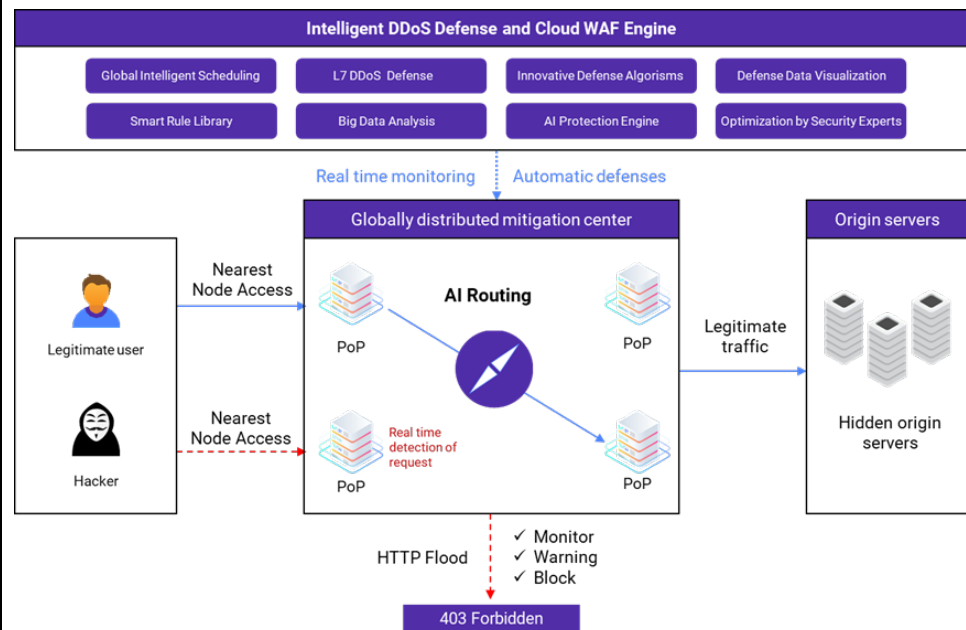
<https://documents.cdnetworks.com/document/15921/appshield-howitworks?rsr=cdnw>

“CDN Pro Global Service Load Balancer (GSLB) inspects the request traffic based on the pre-defined layer 4 and layer 7 policies for any security risks. If the request does not pose a threat, GSLB routes the request to the edge location that best serves the request.”



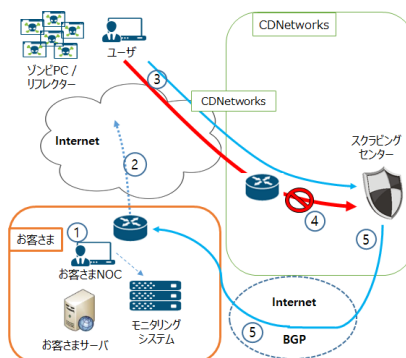
See <https://www.cdnetworks.com/web-performance-blog/cdn-pro-with-waf-for-web-application-protection/>

|  |   |
|--|---|
|  | <p><b>CDNetworks ソリューション適用後</b></p>  <p>■ 状況：DDoSトラフィック発生</p> <ul style="list-style-type: none"> <li>トラフィック方向：       <ul style="list-style-type: none"> <li>- 顧客に向かう通常のトラフィックとDDoSトラフィックはCDNETWORKSネットワークを経由して通信</li> </ul> </li> <li>問題：問題の解決       <ul style="list-style-type: none"> <li>- DDoSトラフィックによる顧客のボトルネックを解消</li> <li>- Dirty Trafficのフィルタリングにより正常ユーザーも接続可能</li> <li>- ファイアウォールやサーバに過負荷を解決</li> <li>- 既存のシステムのIPアドレス変更不要</li> </ul> </li> </ul> <p>■ CDNetworksソリューション導入（事前設定）</p> <ul style="list-style-type: none"> <li>顧客 &lt;-&gt; CDNetworks間BGP構成</li> <li>AS、IP Prefix 広報関連情報設定済み</li> </ul> <p>■ CDNetworksソリューション適用後</p> <ol style="list-style-type: none"> <li>① Customer Monitoring Systemで異常トラフィック検知</li> <li>② 攻撃内容、バイパスするかどうかを判断し、BGPで経路迂回を実施(御客実施)</li> <li>③ トラフィックがCDNetworksに迂回</li> <li>④ Scrubbing CenterでTraffic Cleaning</li> <li>⑤ 通常のトラフィックを事前に構成されたBGPに迂回され顧客ネットワークに配信</li> </ol> <p>1. Detect abnormal traffic by Customer Monitoring System<br/> 2. Determine the content of the attack and whether or not to bypass it, and implement detour using BGP<br/> 3. Divert traffic to CDNetworks<br/> 4. Traffic cleaned at Scrubbing Center<br/> 5. Deliver normal traffic to Customer Network</p> <p><a href="https://pr.cdnetworks.co.jp/blog-ddos-attack-countermeasures-using-gre/">https://pr.cdnetworks.co.jp/blog-ddos-attack-countermeasures-using-gre/</a></p> |
| <p>the enhanced requesting module is further structured, programmed and/or data-communication-connected to apply a first rule to the selected network protocol data collected by the enhanced requesting module; and</p> | <p>CDNetworks analyzes the collected network protocol data to determine whether a DoS attack is occurring.</p> <p><b>“Layer 4 DDoS Mitigation</b><br/> CDN Pro is built upon our Edge Computing Platform. At the entry point of every edge Point of Presence (PoP) is a high-performance Layer 4 distributed denial-of-service (DDoS) firewall. The firewall consists of a group of machines that analyze incoming traffic at line speed. Based on regularly updated rules, the firewall rejects suspicious packets that may endanger services and forwards only the ‘safe’ packets to the servers located behind the firewall. This feature is enabled by default for all edge services and is transparent to all the users.</p> <p><b>Layer 7 DDoS Mitigation</b><br/> The CDN Pro platform monitors the traffic in real-time to detect unusual behaviors at layer 7. Once an attack is identified, defense strategies will be deployed in both layer 4 and layer 7 to most effectively mitigate the impact to normal traffic. Since its inception, CDN Pro has successfully handled some of the world's largest DDoS attacks with bandwidth reaching 1.2Tbps and request rate as high as 35Mrps.”</p> <p><a href="https://docs.cdnetworks.com/en/cdn/docs/recipes/secure-delivery">https://docs.cdnetworks.com/en/cdn/docs/recipes/secure-delivery</a></p>   |



<https://documents.cdnetworks.com/document/15921/appshield-howitworks?rsr=cdnw>

#### CDNetworks ソリューション適用後



#### ・状況：DDoSトラフィック発生

- ・トラフィック方向：顧客に向かう通常のトラフィックとDDoSトラフィックはCDNETWORKSネットワークを経由して通信
- ・問題：問題の解決
  - DDoSトラフィックによる顧客のボトルネックを解消
  - DirtyTrafficのフィルタリングにより正常ユーザーも接続可能
  - ファイアウォールやサーバに過負荷を解決
  - 既存のシステムのIPアドレス変更不要

#### ■ CDNetworksソリューション導入（事前設定）

- ・顧客 < - > CDNetworks間EBGP構成
- ・AS、IP Prefix 広報関連情報設定済み

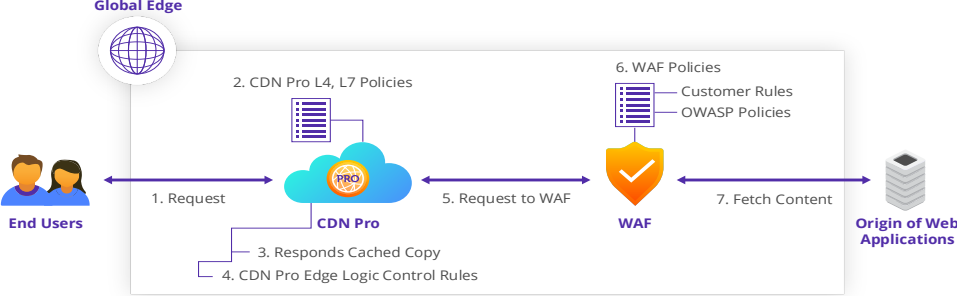
#### ■ CDNetworksソリューション適用後

- ① Customer Monitoring Systemで異常トラフィック検知
- ② 攻撃内容、バイパスするかどうかを判断し、BGPで経路迂回を実施(御客実施)
- ③ トラフィックがCDNetworksに迂回
- ④ Scrubbing CenterでTraffic Cleaning
- ⑤ 通常のトラフィックを事前に構成されたBGPに迂回され顧客ネットワークに配信

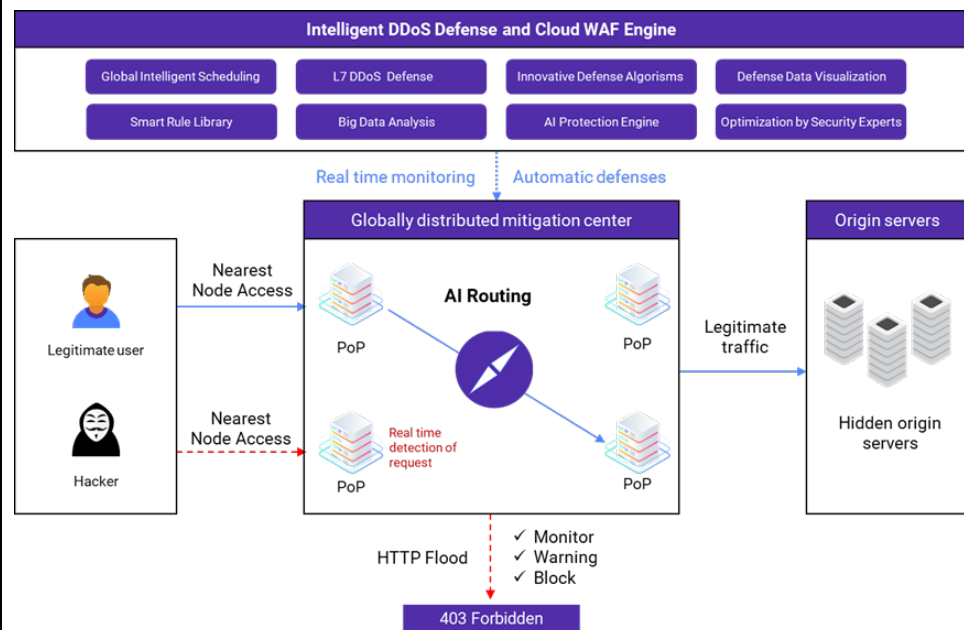
1. Detect abnormal traffic by Customer Monitoring System
2. Determine the content of the attack and whether or not to bypass it, and implement detour using BGP
3. Divert traffic to CDNetworks
4. Traffic cleaned at Scrubbing Center
5. Deliver normal traffic to Customer Network

<https://pr.cdnetworks.co.jp/blog-ddos-attack-countermeasures-using-gre/>

“CDN Pro Global Service Load Balancer (GSLB) inspects the request traffic based on the pre-defined layer 4 and layer 7 policies for any security risks. If the request does not pose a threat, GSLB routes the request to the edge location that best serves the request.”

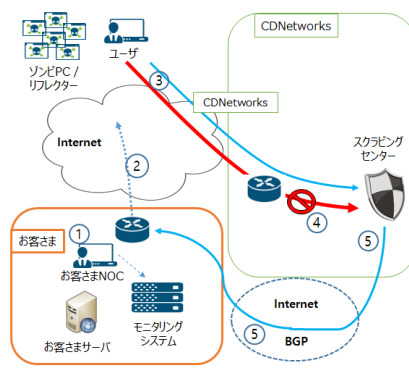
|  |   |
|--|---|
|  |  <p>See <a href="https://www.cdnetworks.com/web-performance-blog/cdn-pro-with-waf-for-web-application-protection/">https://www.cdnetworks.com/web-performance-blog/cdn-pro-with-waf-for-web-application-protection/</a></p> <p>“Policies include IP/URL blacklist and whitelist, access control by IP address, URL, domain name.”<br/>CDNetworks-DDoS-Product-Overview.pdf</p>  |
| <p>the enhanced requesting module is further structured, programmed and/or data-communication-connected to selectively make a responsive reaction based, at least in part, upon the application of the first rule by the enhanced requesting module to the selected network protocol data.</p> | <p>If a DoS attack is detected based on the analysis of the collected network protocol data, CDNetworks does not deliver potentially data packets directly to the customer network but, instead, re-routes suspect packets to a Scrubbing Center or blocks them altogether.</p> <p><u>“Layer 4 DDoS Mitigation</u><br/>CDN Pro is built upon our Edge Computing Platform. At the entry point of every edge Point of Presence (PoP) is a high-performance Layer 4 distributed denial-of-service (DDoS) firewall. The firewall consists of a group of machines that analyze incoming traffic at line speed. Based on regularly updated rules, the firewall rejects suspicious packets that may endanger services and forwards only the ‘safe’ packets to the servers located behind the firewall. This feature is enabled by default for all edge services and is transparent to all the users.</p> <p><u>Layer 7 DDoS Mitigation</u><br/>The CDN Pro platform monitors the traffic in real-time to detect unusual behaviors at layer 7. Once an attack is identified, defense strategies will be deployed in both layer 4 and layer 7 to most effectively mitigate the impact to normal traffic. Since its inception, CDN Pro has successfully handled some of the world's largest DDoS attacks with bandwidth reaching 1.2Tbps and request rate as high as 35Mrps.”<br/><a href="https://docs.cdnetworks.com/en/cdn/docs/recipes/secure-delivery">https://docs.cdnetworks.com/en/cdn/docs/recipes/secure-delivery</a></p> |





<https://documents.cdnetworks.com/document/15921/appshield-howitworks?rsr=cdnw>

#### CDNetworks ソリューション適用後



・ 状況：DDoSトラフィック発生

・ トラフィック方向：  
- 顧客に向かう通常のトラフィックとDDoSトラフィックはCDNETWORKSネットワークを経由して通信

・ 問題：問題の解決  
- DDoSトラフィックによる顧客のボトルネックを解消  
- Dirty Trafficのフィルタリングにより正常ユーザーも接続可能  
- ファイアウォールやサーバに過負荷を解決  
- 既存のシステムのIPアドレス変更不要

#### ■ CDNetworksソリューション導入（事前設定）

・ 顧客 <-> CDNetworks間EBGP構成  
・ AS、IP Prefix 広報関連情報設定済み

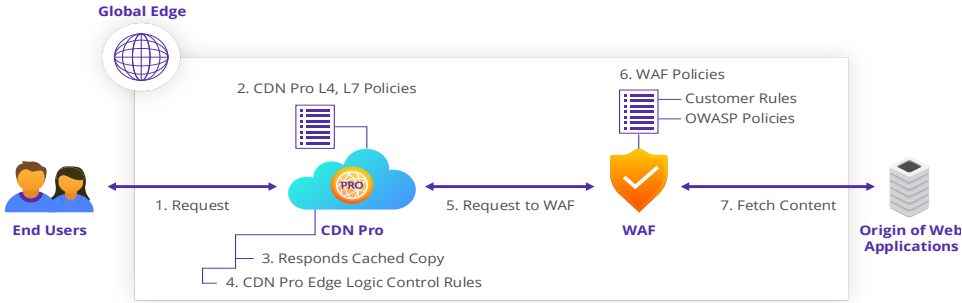
#### ■ CDNetworksソリューション適用後

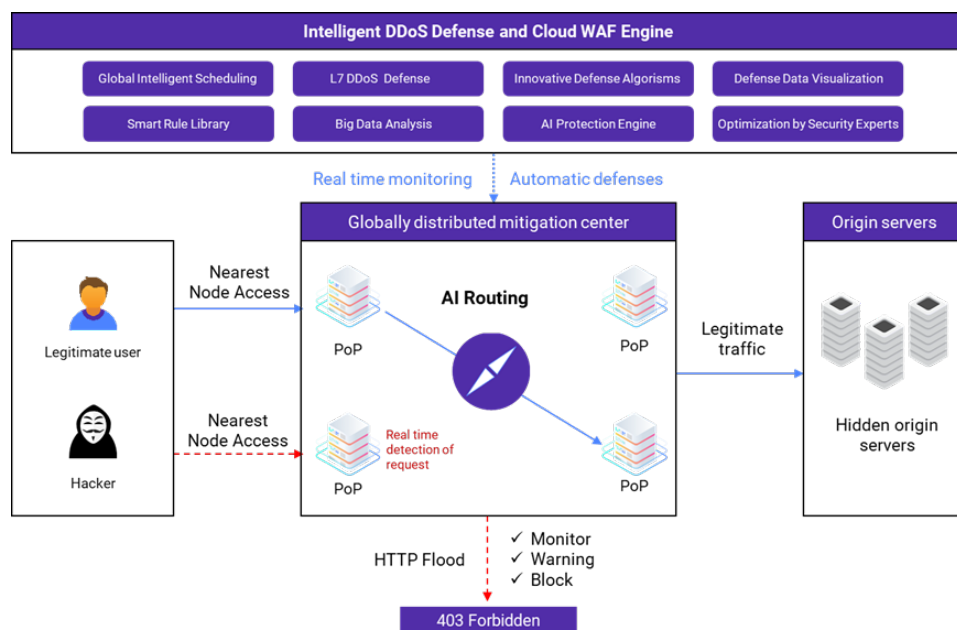
① Customer Monitoring Systemで異常トラフィック検知  
② 攻撃内容、バイパスするかどうかを判断し、BGPで経路迂回を実施(御客実施)  
③ トラフィックがCDNetworksに迂回  
④ Scrubbing CenterでTraffic Cleaning  
⑤ 通常のトラフィックを事前に構成されたBGPに迂回され顧客ネットワークに配信

1. Detect abnormal traffic by Customer Monitoring System
2. Determine the content of the attack and whether or not to bypass it, and implement detour using BGP
3. Divert traffic to CDNetworks
4. Traffic cleaned at Scrubbing Center
5. Deliver normal traffic to Customer Network

<https://pr.cdnetworks.co.jp/blog-ddos-attack-countermeasures-using-gre/>

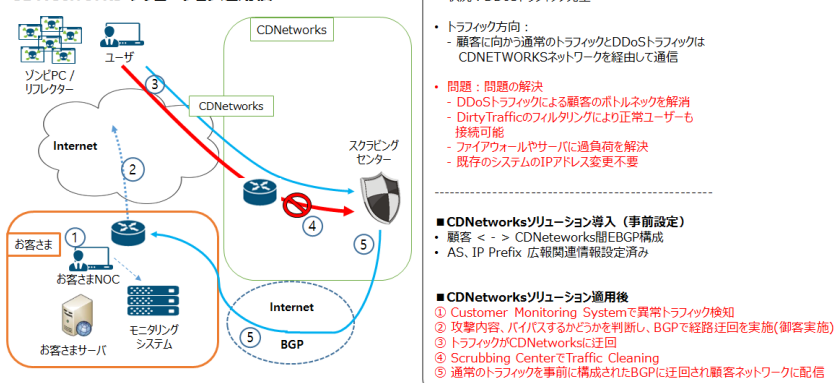
“CDN Pro Global Service Load Balancer (GSLB) inspects the request traffic based on the pre-defined layer 4 and layer 7 policies for any

|   |  |
|---|--|
|   | <p>security risks. If the request does not pose a threat, GSLB routes the request to the edge location that best serves the request.”</p>  <p>See <a href="https://www.cdnetworks.com/web-performance-blog/cdn-pro-with-waf-for-web-application-protection/">https://www.cdnetworks.com/web-performance-blog/cdn-pro-with-waf-for-web-application-protection/</a></p> <p>“Policies include IP/URL blacklist and whitelist, access control by IP address, URL, domain name.”<br/>CDNetworks-DDoS-Product-Overview.pdf</p>   |
| <p>10. The gateway of claim 7, wherein the responsive reaction made by the gateway includes one or more of the following types of responsive reactions: (i) filtering the first DU so that it is selectively not communicated to the connectionless network, (ii) regulating communication of the first DU to the connectionless network, (iii) reallocating network resources of the system, and/or (iv) sending out an alert.</p> | <p>If a DoS attack is detected based on the analysis of the collected network protocol data, CDNetworks does not deliver potentially data packets directly to the customer network but, instead, re-routes suspect packets to a Scrubbing Center or blocks them altogether. CDNetworks also notifies the customer of the suspected attack.</p> <p><u>“Layer 4 DDoS Mitigation</u><br/>CDN Pro is built upon our Edge Computing Platform. At the entry point of every edge Point of Presence (PoP) is a high-performance Layer 4 distributed denial-of-service (DDoS) firewall. The firewall consists of a group of machines that analyze incoming traffic at line speed. Based on regularly updated rules, the firewall rejects suspicious packets that may endanger services and forwards only the ‘safe’ packets to the servers located behind the firewall. This feature is enabled by default for all edge services and is transparent to all the users.</p> <p><u>Layer 7 DDoS Mitigation</u><br/>The CDN Pro platform monitors the traffic in real-time to detect unusual behaviors at layer 7. Once an attack is identified, defense strategies will be deployed in both layer 4 and layer 7 to most effectively mitigate the impact to normal traffic. Since its inception, CDN Pro has successfully handled some of the world's largest DDoS attacks with bandwidth reaching 1.2Tbps and request rate as high as 35Mrps.”<br/><a href="https://docs.cdnetworks.com/en/cdn/docs/recipes/secure-delivery">https://docs.cdnetworks.com/en/cdn/docs/recipes/secure-delivery</a></p> |



<https://documents.cdnetworks.com/document/15921/appshield-howitworks?rsr=cdnw>

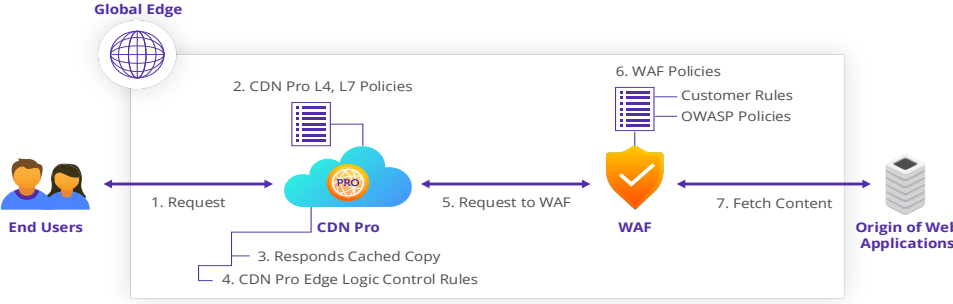
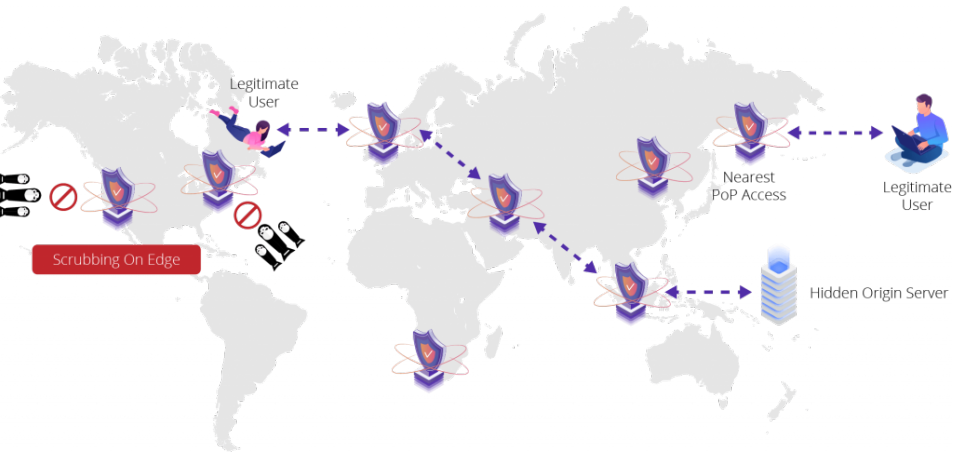
#### CDNetworks ソリューション適用後



1. Detect abnormal traffic by Customer Monitoring System
2. Determine the content of the attack and whether or not to bypass it, and implement detour using BGP
3. Divert traffic to CDNetworks
4. Traffic cleaned at Scrubbing Center
5. Deliver normal traffic to Customer Network

<https://pr.cdnetworks.co.jp/blog-ddos-attack-countermeasures-using-gre/>

“CDN Pro Global Service Load Balancer (GSLB) inspects the request traffic based on the pre-defined layer 4 and layer 7 policies for any security risks. If the request does not pose a threat, GSLB routes the request to the edge location that best serves the request.”

|  |   |
|--|---|
|  |  <p>See <a href="https://www.cdnetworks.com/web-performance-blog/cdn-pro-with-waf-for-web-application-protection/">https://www.cdnetworks.com/web-performance-blog/cdn-pro-with-waf-for-web-application-protection/</a></p>   |
| <p>20. A method of communicating a data unit through a computer communication network system, the method comprising the following steps:</p> | <p>CDNetworks delivers websites and web applications to over 99% of the world within milliseconds with its global content delivery network of over 200,000 servers and over 2,800 global Points of Presence (PoPs).<br/> <a href="https://www.cdnetworks.com/">https://www.cdnetworks.com/</a></p>  |
| <p>receiving, by a gateway, a first MPDU from a connection-based network of the computer communication network system;</p>                   | <p>CDNetworks connects customer end-users to the internet (a connection-based network). Data packets (MPDUs) being sent to a customer end-user enter the network through an edge router (a gateway) at a CDNetwork Point-of-Presence.</p>  <p>See <a href="https://www.cdnetworks.com/cloud-security/flood-shield/">https://www.cdnetworks.com/cloud-security/flood-shield/</a></p> <p>“Flood Shield DDoS deflection technology is deployed on CDNetworks’ distributed Points-of-Presence (PoPs). It is a cloud-based ‘always-on’ mitigation service with virtually unlimited capacity.”<br/> <a href="https://www.cdnetworks.com/cloud-security/flood-shield/">https://www.cdnetworks.com/cloud-security/flood-shield/</a></p> |

“Flood Shield is deployed on CDNetworks’ huge global infrastructure with data centers in the USA, Europe, Asia, and mainland China. With over 12 global DDoS scrubbing centers and 15Tbps of total capacity, it is designed to protect websites and network infrastructures against even the most sophisticated and large-scale volumetric attacks.”

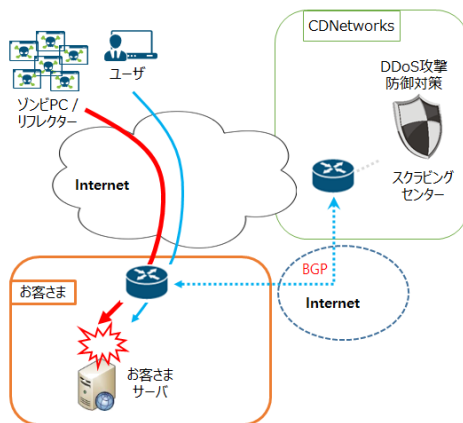
<https://www.cdnetworks.com/cloud-security/flood-shield/>

“Flood Shield is deployed on CDNetworks’ distributed Points-of-Presence (PoPs). It is a cloud-based ‘always on’ solution with virtually unlimited capacity. It does not require sophisticated deployments and changes to customers’ network and provides automated transparent scaling.

Flood Shield is provided either via a simple DNS change, typically to protect web sites and HTTP/S traffic, or through an anycast IP in order to protect entire network infrastructures, including multiple domains, servers and protocols. With the customers’ traffic routed through CDNetworks’ PoPs, DDoS attacks hit the CDNetwork infrastructure rather than our customers’ servers and networks. CDNetworks’ PoPs detect and deflect both application-layer attacks (L7) and all known types of network-layer attacks (L3/L4), including Ack and Syn floods, UDP floods, ICMP floods, CC attacks and more.”

<https://documents.cdnetworks.com/document/15920/floodshield-how-it-work>

#### CDNetworksソリューション導入（事前設定）



- ・ 状況：DDoSトラフィック発生
- ・ トラフィックの方向：
  - 顧客に向かう通常のトラフィックと
  - DDoSトラフィックが既存ネットワーク経由で通信
- ・ 問題：
  - DDoSトラフィックにより、ネットワークボトルネック発生
  - ボトルネックが原因で、通常のユーザーも接続不可
  - ファイアウォールやサーバに過負荷が発生

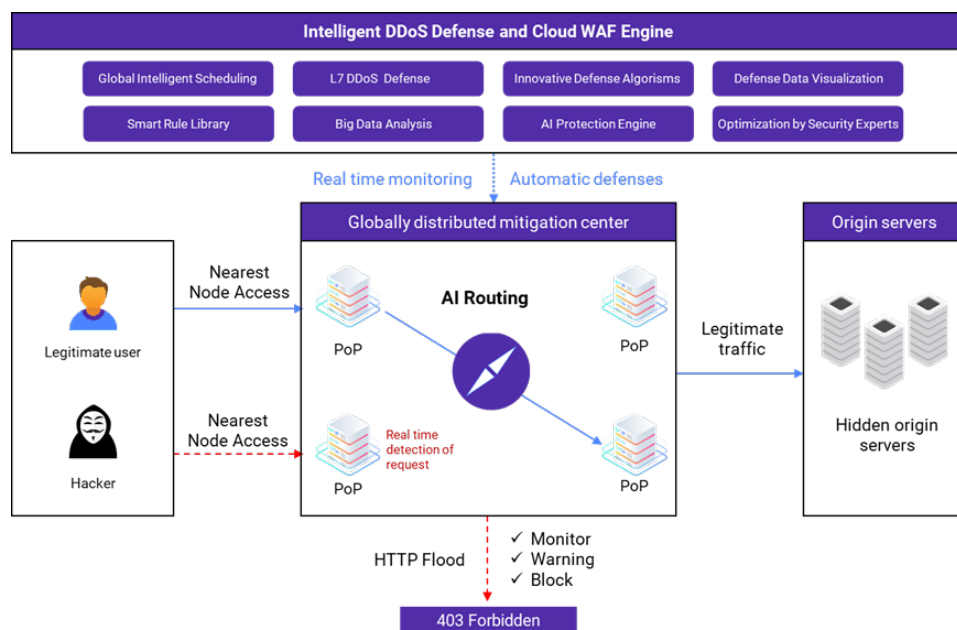
#### ■ CDNetworksソリューション導入（事前設定）

- ・ 顧客 < - > CDNetworks間EBGP構成
- ・ AS、IP関連情報設定
- ・ 顧客AS、IP 広報を行う

<https://pr.cdnetworks.co.jp/blog-ddos-attack-countermeasures-using-gre/>

BGP = Border Gateway Protocol

EBGP = External BGP; for communication between two Autonomous Systems (e.g., CDNetworks’ network and customer’s network)



<https://documents.cdnetworks.com/document/15921/appshield-howitworks?rsr=cdnw>

CDNetworks has PoPs located in Ashburn, VA; Boston, MA; Chicago, IL; Dallas, TX; Denver, CO; Los Angeles, CA; Miami, FL; New York, NY; San Jose, CA; and Seattle, WA

See <https://www.cdnetworks.com/cdnpro-pricing/>

CDNetworks has scrubbing centers located in New York, NY and Los Angeles, CA. See <https://www.cdnetworks.com/about/global-network-map/>

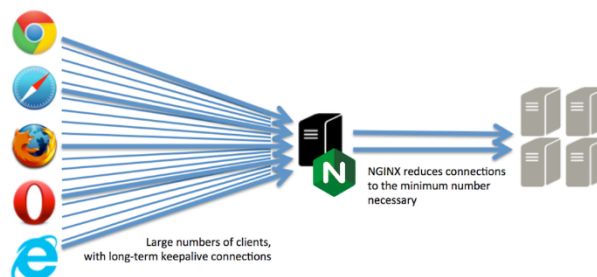
CDNetworks has points-of-presence and/or edge computing sites in Texas are located at 6653 Pinecrest Drive, Plano, Texas 75024 and 1950 N Stemmons Freeway, Dallas, Texas 75207.

disaggregating, by the gateway, the first MPDU into a plurality of smaller data units (DUs);

CDNetworks' edge routers receive packets (MPDUs) from the internet (a connection-based network), disaggregate/demux those packets into smaller packets (smaller DUs), and communicate the smaller packets to a target network (a receiver-side connectionless network).

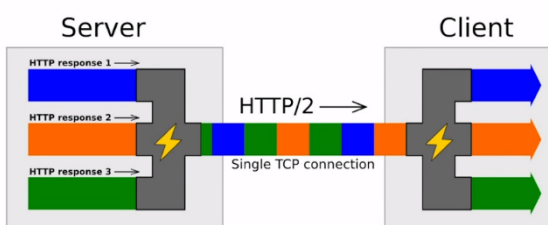
"CDN Pro is a serverless Nginx Platform with control at the Edge, built-in security, and real-time acceleration for optimizing websites, APIs, and cloud applications."

<https://www.cdnetworks.com/cdnpro/>



<https://www.nginx.com/blog/load-balancing-with-nginx-plus-part-2/>

### HTTP/2 Inside: multiplexing



“The next key point of HTTP/2 is multiplexing. Instead of sending and receiving responses and requests as separate streams of data over multiple connections, HTTP/2 multiplexes them over one stream of bytes or one stream of data.”

<https://www.nginx.com/blog/http2-module-nginx/>

collecting, by the gateway, selected network protocol data from the first MPDU, with the selected network protocol data including at least some network protocol data included in the first MPDU and not included in any of the plurality of DUs, and with the selected network protocol data

CDNetworks collects network protocol data, such as IP addresses, from incoming data packets received from the internet. None of this network protocol data includes data from the packet payload.

“CDNetworks content delivery networks (CDN) serves thousands of large global enterprises, process TB-scale log data daily, including a massive access data and attack/defense samples. The platform’s big data and machine learning capabilities help detect network attack trends in real-time and automatically activates defense in advance. It also intelligently analyzes and identifies attacks, to model the normal behaviors of legitimate traffic including IP addresses, HTTP headers, cookies, and JavaScript snippets, etc.”

<https://www.cdnetworks.com/cloud-security/flood-shield/>

### “Layer 4 DDoS Mitigation

CDN Pro is built upon our Edge Computing Platform. At the entry point of every edge Point of Presence (PoP) is a high-performance Layer 4



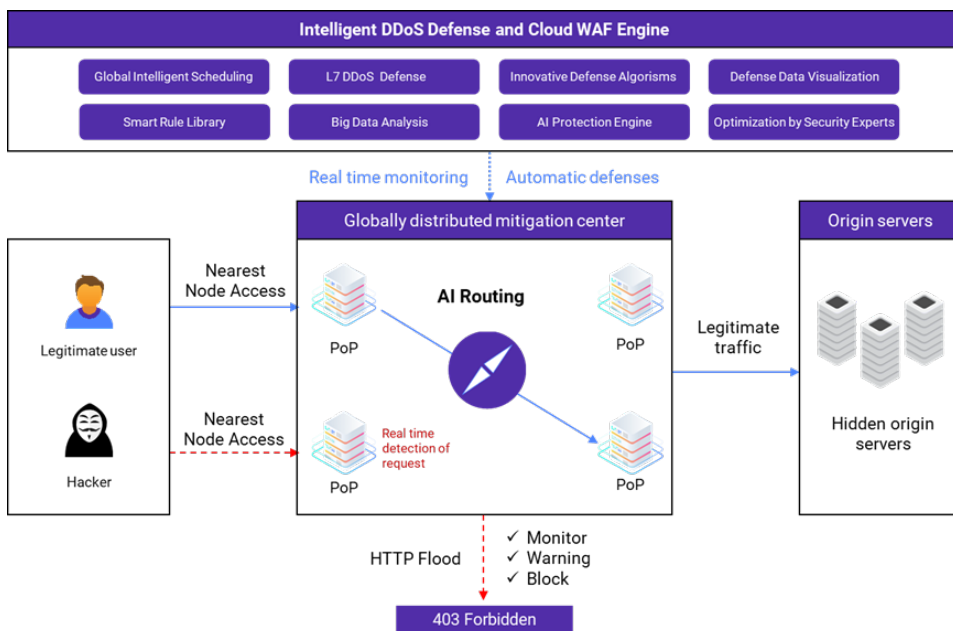
relating exclusively to network protocols and including no data from any data payload(s) which may be present in the MPDU;

distributed denial-of-service (DDoS) firewall. The firewall consists of a group of machines that analyze incoming traffic at line speed. Based on regularly updated rules, the firewall rejects suspicious packets that may endanger services and forwards only the 'safe' packets to the servers located behind the firewall. This feature is enabled by default for all edge services and is transparent to all the users.

#### Layer 7 DDoS Mitigation

The CDN Pro platform monitors the traffic in real-time to detect unusual behaviors at layer 7. Once an attack is identified, defense strategies will be deployed in both layer 4 and layer 7 to most effectively mitigate the impact to normal traffic. Since its inception, CDN Pro has successfully handled some of the world's largest DDoS attacks with bandwidth reaching 1.2Tbps and request rate as high as 35Mrps."

<https://docs.cdnetworks.com/en/cdn/docs/recipes/secure-delivery>



<https://documents.cdnetworks.com/document/15921/appshield-howitworks?rsr=cdnw>



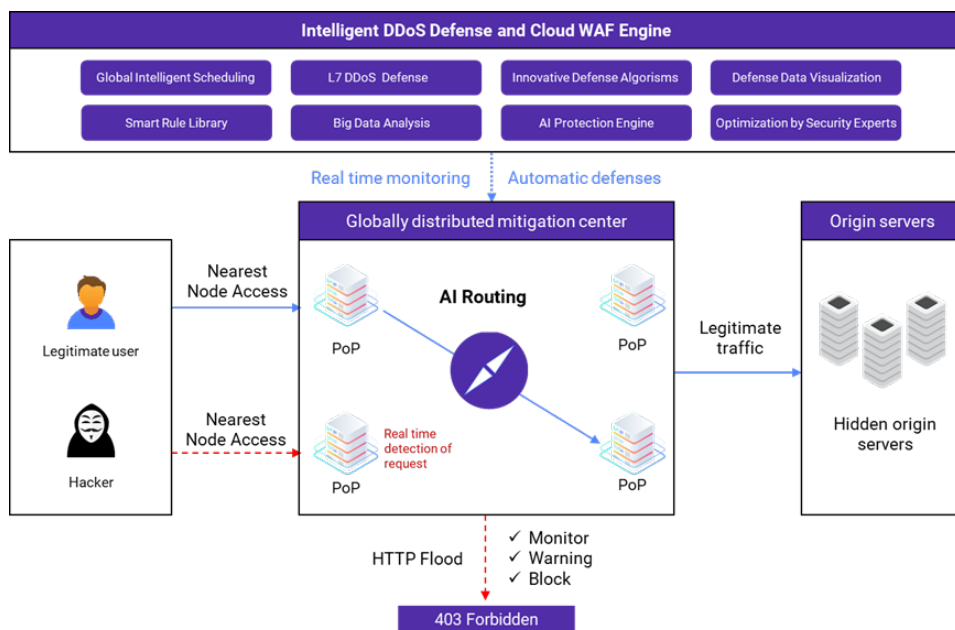
|  |  |
|--|--|
|  | <p><b>CDNetworks ソリューション適用後</b></p> <p>・ 状況：DDoSトラフィック発生</p> <p>・ トラフィック方向：<br/>- 顧客に向かう通常のトラフィックとDDoSトラフィックはCDNETWORKSネットワークを経由して通信</p> <p>・ 問題：問題の解決<br/>- DDoSトラフィックによる顧客のボトルネックを解消<br/>- Dirty Trafficのフィルタリングにより正常ユーザーも接続可能<br/>- ファイアウォールやサーバに過負荷を解決<br/>- 既存のシステムのIPアドレス変更不要</p> <p>■ CDNetworksソリューション導入（事前設定）<br/>・ 顧客 &lt;-&gt; CDNetworks間EBGP構成<br/>・ AS、IP Prefix 広報関連情報設定済み</p> <p>■ CDNetworksソリューション適用後<br/>① Customer Monitoring Systemで異常トラフィック検知<br/>② 攻撃内容、バイパスするかどうかを判断し、BGPで経路迂回を実施(御客実施)<br/>③ トラフィックがCDNetworksに迂回<br/>④ Scrubbing CenterでTraffic Cleaning<br/>⑤ 通常のトラフィックを事前に構成されたBGPに迂回され顧客ネットワークに配信</p> <p>1. Detect abnormal traffic by Customer Monitoring System<br/>2. Determine the content of the attack and whether or not to bypass it, and implement detour using BGP<br/>3. Divert traffic to CDNetworks<br/>4. Traffic cleaned at Scrubbing Center<br/>5. Deliver normal traffic to Customer Network</p> <p><a href="https://pr.cdnetworks.co.jp/blog-ddos-attack-countermeasures-using-gre/">https://pr.cdnetworks.co.jp/blog-ddos-attack-countermeasures-using-gre/</a></p> <p>“CDN Pro Global Service Load Balancer (GSLB) inspects the request traffic based on the pre-defined layer 4 and layer 7 policies for any security risks. If the request does not pose a threat, GSLB routes the request to the edge location that best serves the request.”</p> <p>See <a href="https://www.cdnetworks.com/web-performance-blog/cdn-pro-with-waf-for-web-application-protection/">https://www.cdnetworks.com/web-performance-blog/cdn-pro-with-waf-for-web-application-protection/</a></p> |
| <p>applying, by the gateway, a first rule to the selected network protocol data;</p> | <p>CDNetworks analyzes the collected network protocol data to determine whether a DoS attack is occurring.</p> <p><b>“Layer 4 DDoS Mitigation</b><br/>CDN Pro is built upon our Edge Computing Platform. At the entry point of every edge Point of Presence (PoP) is a high-performance Layer 4 distributed denial-of-service (DDoS) firewall. The firewall consists of a group of machines that analyze incoming traffic at line speed. Based on</p>  |

regularly updated rules, the firewall rejects suspicious packets that may endanger services and forwards only the 'safe' packets to the servers located behind the firewall. This feature is enabled by default for all edge services and is transparent to all the users.

#### Layer 7 DDoS Mitigation

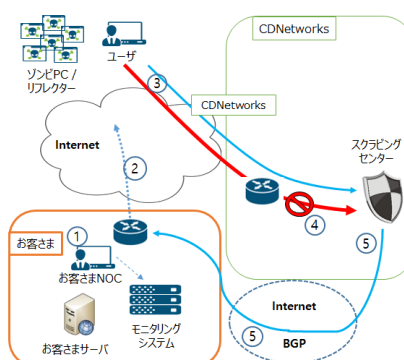
The CDN Pro platform monitors the traffic in real-time to detect unusual behaviors at layer 7. Once an attack is identified, defense strategies will be deployed in both layer 4 and layer 7 to most effectively mitigate the impact to normal traffic. Since its inception, CDN Pro has successfully handled some of the world's largest DDoS attacks with bandwidth reaching 1.2Tbps and request rate as high as 35Mrps."

<https://docs.cdnetworks.com/en/cdn/docs/recipes/secure-delivery>



<https://documents.cdnetworks.com/document/15921/appshield-howitworks?rsr=cdnw>

## CDNetworks ソリューション適用後



・ 状況：DDoSトラフィック発生

・ トラフィック方向：  
- 顧客に向かう通常のトラフィックとDDoSトラフィックはCDNETWORKSネットワークを経由して通信

・ 問題：問題の解決  
- DDoSトラフィックによる顧客のポトルネックを解消  
- Dirty Trafficのフィルタリングにより正常ユーザーも接続可能  
- ファイアウォールやサーバに過負荷を解決  
- 既存のシステムのIPアドレス変更不要

## ■ CDNetworksソリューション導入（事前設定）

・ 顧客 < - > CDNetworks間EBGP構成  
・ AS、IP Prefix 広範囲連携情報設定済み

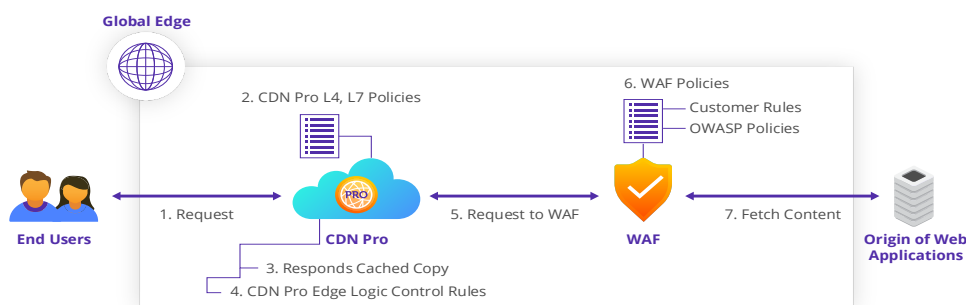
## ■ CDNetworksソリューション適用後

① Customer Monitoring Systemで異常トラフィック検知  
② 攻撃内容、バイパスするかどうかを判断し、BGPで経路迂回を実施(御客実施)  
③ トラフィックがCDNetworksに迂回  
④ Scrubbing CenterでTraffic Cleaning  
⑤ 通常のトラフィックを事前に構成されたBGPに迂回され顧客ネットワークに配信

1. Detect abnormal traffic by Customer Monitoring System
2. Determine the content of the attack and whether or not to bypass it, and implement detour using BGP
3. Divert traffic to CDNetworks
4. Traffic cleaned at Scrubbing Center
5. Deliver normal traffic to Customer Network

<https://pr.cdnetworks.co.jp/blog-ddos-attack-countermeasures-using-gre/>

“CDN Pro Global Service Load Balancer (GSLB) inspects the request traffic based on the pre-defined layer 4 and layer 7 policies for any security risks. If the request does not pose a threat, GSLB routes the request to the edge location that best serves the request.”



See <https://www.cdnetworks.com/web-performance-blog/cdn-pro-with-waf-for-web-application-protection/>

“Policies include IP/URL blacklist and whitelist, access control by IP address, URL, domain name.”

CDNetworks-DDoS-Product-Overview.pdf

selectively making, by the gateway, a responsive reaction based, at least in

If a DoS attack is detected based on the analysis of the collected network protocol data, CDNetworks does not deliver potentially data packets directly to the customer network but, instead, re-routes suspect packets to a Scrubbing Center or blocks them altogether.

part, upon the application of the first rule to the selected network protocol data at the applying step; and

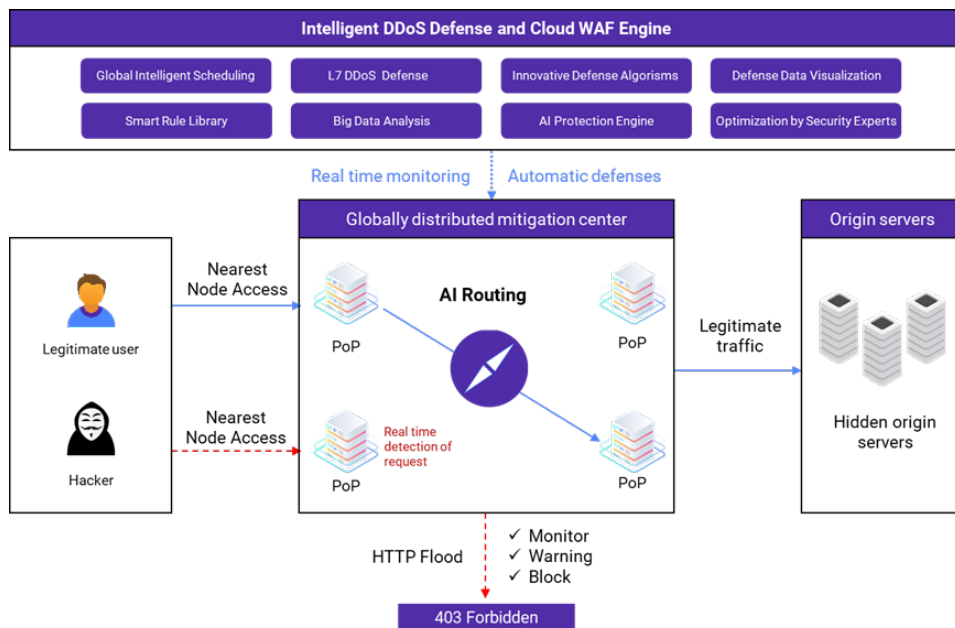
#### “Layer 4 DDoS Mitigation

CDN Pro is built upon our Edge Computing Platform. At the entry point of every edge Point of Presence (PoP) is a high-performance Layer 4 distributed denial-of-service (DDoS) firewall. The firewall consists of a group of machines that analyze incoming traffic at line speed. Based on regularly updated rules, the firewall rejects suspicious packets that may endanger services and forwards only the ‘safe’ packets to the servers located behind the firewall. This feature is enabled by default for all edge services and is transparent to all the users.

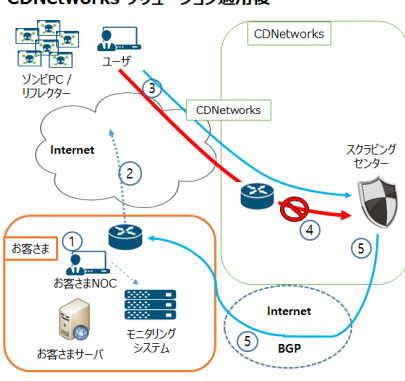
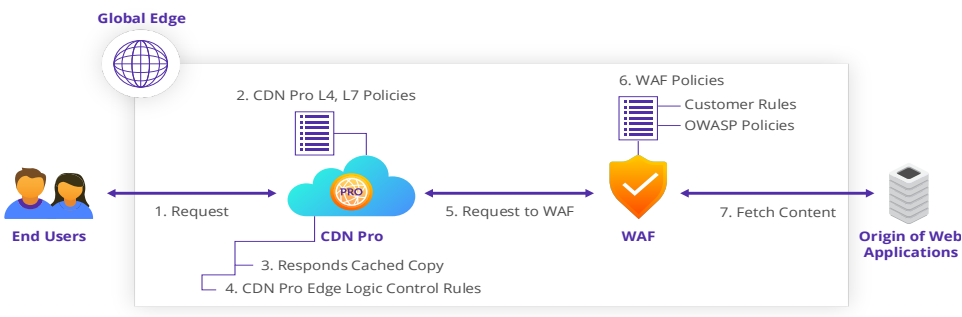
#### Layer 7 DDoS Mitigation

The CDN Pro platform monitors the traffic in real-time to detect unusual behaviors at layer 7. Once an attack is identified, defense strategies will be deployed in both layer 4 and layer 7 to most effectively mitigate the impact to normal traffic. Since its inception, CDN Pro has successfully handled some of the world's largest DDoS attacks with bandwidth reaching 1.2Tbps and request rate as high as 35Mrps.”

<https://docs.cdnetworks.com/en/cdn/docs/recipes/secure-delivery>



<https://documents.cdnetworks.com/document/15921/appshield-howitworks?rsr=cdnw>

|  |  |
|--|--|
|  | <p><b>CDNetworks ソリューション適用後</b></p>  <ul style="list-style-type: none"> <li>・ 状況：DDoSトラフィック発生</li> <li>・ トラフィック方向：             <ul style="list-style-type: none"> <li>- 顧客に向かう通常のトラフィックとDDoSトラフィックはCDNETWORKSネットワークを経由して通信</li> </ul> </li> <li>・ 問題：問題の解決             <ul style="list-style-type: none"> <li>- DDoSトラフィックによる顧客のボトルネックを解消</li> <li>- Dirty Trafficのフィルタリングにより正常ユーザーも接続可能</li> <li>- ファイアウォールやサーバに過負荷を解決</li> <li>- 既存のシステムのIPアドレス変更不要</li> </ul> </li> <li>■ CDNetworksソリューション導入（事前設定）             <ul style="list-style-type: none"> <li>・ 顧客 &lt; - &gt; CDNetworks間EBGP構成</li> <li>・ AS、IP Prefix 広範囲連情報設定済み</li> </ul> </li> <li>■ CDNetworksソリューション適用後             <ol style="list-style-type: none"> <li>① Customer Monitoring Systemで異常トラフィック検知</li> <li>② 攻撃内容、バイパスするかどうかを判断し、BGPで経路迂回を実施(御客実施)</li> <li>③ トラフィックがCDNetworksに迂回</li> <li>④ Scrubbing CenterでTraffic Cleaning</li> <li>⑤ 通常のトラフィックを事前に構成されたBGPに迂回され顧客ネットワークに配信</li> </ol> </li> </ul> <p>1. Detect abnormal traffic by Customer Monitoring System<br/>         2. Determine the content of the attack and whether or not to bypass it, and implement detour using BGP<br/>         3. Divert traffic to CDNetworks<br/>         4. Traffic cleaned at Scrubbing Center<br/>         5. Deliver normal traffic to Customer Network</p> <p><a href="https://pr.cdnetworks.co.jp/blog-ddos-attack-countermeasures-using-gre/">https://pr.cdnetworks.co.jp/blog-ddos-attack-countermeasures-using-gre/</a></p> <p>“CDN Pro Global Service Load Balancer (GSLB) inspects the request traffic based on the pre-defined layer 4 and layer 7 policies for any security risks. If the request does not pose a threat, GSLB routes the request to the edge location that best serves the request.”</p>  <p>See <a href="https://www.cdnetworks.com/web-performance-blog/cdn-pro-with-waf-for-web-application-protection/">https://www.cdnetworks.com/web-performance-blog/cdn-pro-with-waf-for-web-application-protection/</a></p> <p>“Policies include IP/URL blacklist and whitelist, access control by IP address, URL, domain name.”<br/>         CDNetworks-DDoS-Product-Overview.pdf</p> |
| selectively communicating, by the gateway, the first DU to a | If a DoS attack is detected based on the analysis of the collected network protocol data, CDNetworks does not deliver potentially data packets directly to the customer network but, instead, re-routes suspect packets to a Scrubbing Center or blocks them altogether.   |

receiver-side connectionless network of the computer communication network system on condition that the communicating of the first DU does not conflict with the responsive reaction of the selectively communicating step.

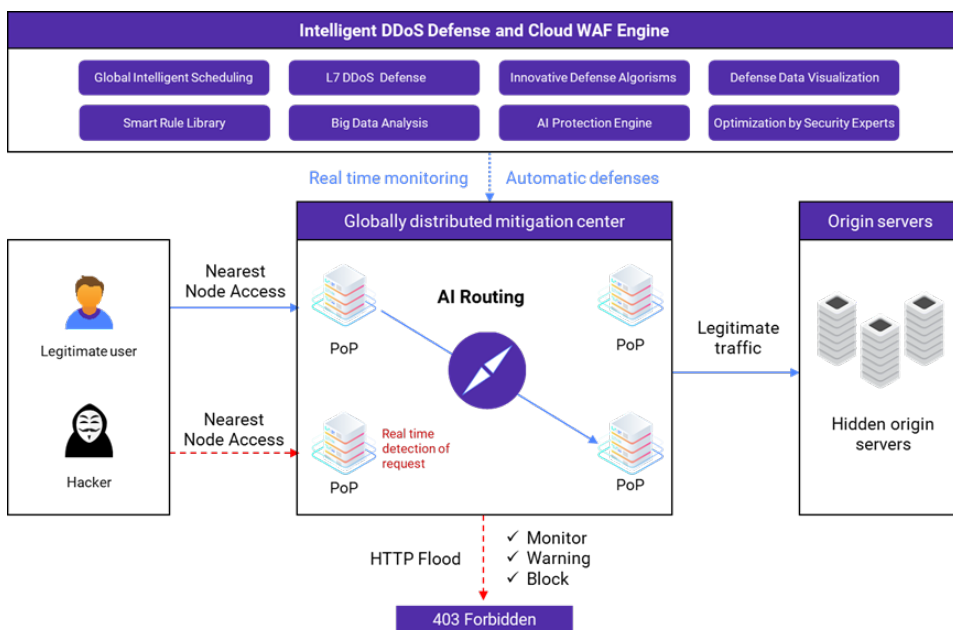
#### “Layer 4 DDoS Mitigation

CDN Pro is built upon our Edge Computing Platform. At the entry point of every edge Point of Presence (PoP) is a high-performance Layer 4 distributed denial-of-service (DDoS) firewall. The firewall consists of a group of machines that analyze incoming traffic at line speed. Based on regularly updated rules, the firewall rejects suspicious packets that may endanger services and forwards only the ‘safe’ packets to the servers located behind the firewall. This feature is enabled by default for all edge services and is transparent to all the users.

#### Layer 7 DDoS Mitigation

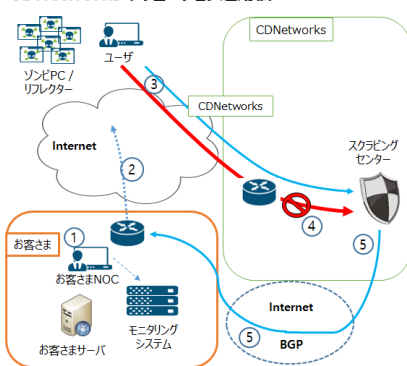
The CDN Pro platform monitors the traffic in real-time to detect unusual behaviors at layer 7. Once an attack is identified, defense strategies will be deployed in both layer 4 and layer 7 to most effectively mitigate the impact to normal traffic. Since its inception, CDN Pro has successfully handled some of the world's largest DDoS attacks with bandwidth reaching 1.2Tbps and request rate as high as 35Mrps.”

<https://docs.cdnetworks.com/en/cdn/docs/recipes/secure-delivery>



<https://documents.cdnetworks.com/document/15921/appshield-howitworks?rsr=cdnw>

## CDNetworks ソリューション適用後



・ 状況：DDoSトラフィック発生

・ トラフィック方向：  
- 顧客に向かう通常のトラフィックとDDoSトラフィックは  
CDNETWORKSネットワークを経由して通信

・ 問題：問題の解決

- DDoSトラフィックによる顧客のポトルネックを解消  
- DirtyTrafficのフィルタリングにより正常ユーザーも  
接続可能  
- ファイアウォールやサーバに過負荷を解決  
- 既存のシステムのIPアドレス変更不要

## ■ CDNetworksソリューション導入（事前設定）

・ 顧客 < - > CDNetworks間EBGP構成  
・ AS, IP Prefix 広報関連情報設定済み

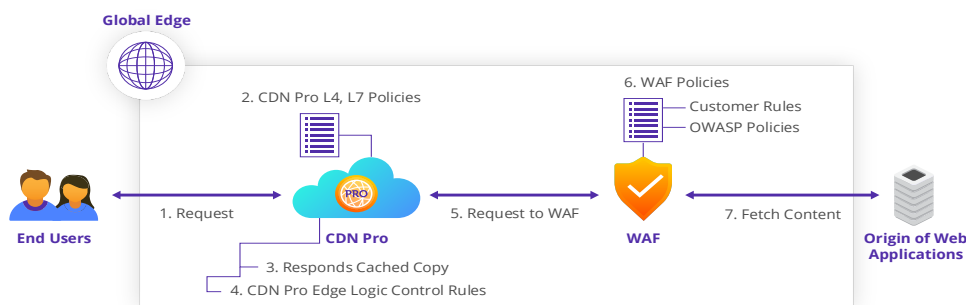
## ■ CDNetworksソリューション適用後

① Customer Monitoring Systemで異常トラフィック検知  
② 攻撃内容、バイパスするかどうかを判断し、BGPで経路迂回を実施(御客実施)  
③ トラフィックがCDNetworksに迂回  
④ Scrubbing CenterでTraffic Cleaning  
⑤ 通常のトラフィックを事前に構成されたBGPに迂回され顧客ネットワークに配信

1. Detect abnormal traffic by Customer Monitoring System
2. Determine the content of the attack and whether or not to bypass it, and implement detour using BGP
3. Divert traffic to CDNetworks
4. Traffic cleaned at Scrubbing Center
5. Deliver normal traffic to Customer Network

<https://pr.cdnetworks.co.jp/blog-ddos-attack-countermeasures-using-gre/>

“CDN Pro Global Service Load Balancer (GSLB) inspects the request traffic based on the pre-defined layer 4 and layer 7 policies for any security risks. If the request does not pose a threat, GSLB routes the request to the edge location that best serves the request.”



See <https://www.cdnetworks.com/web-performance-blog/cdn-pro-with-waf-for-web-application-protection/>